

CLAIMS

What is claimed is:

- 1 1. A method for secure communications in a computer network,
2 comprising;
3 combining individually encrypted network security protection
4 handshake messages into a set of encrypted messages wherein each encrypted
5 handshake message is derived using a public key containing an encryption
6 exponent;
7 determining a root node of a binary tree comprising leaf nodes
8 corresponding to each encryption exponent;
9 calculating a product of the encrypted messages;
10 extracting at least one root from the product of the encrypted messages;
11 and
12 decrypting the encrypted messages by expressing the at least one root as
13 at least one promise and evaluating the at least one promise at the leaf nodes
14 decreasing the number of modular inversions wherein efficiency of the
15 decryption is increased.
- 1 2. The method of claim 1, wherein the secure communications
2 include secure socket layer ("SSL") messages.

1 3. The method of claim 1, wherein the secure communications
2 include transport layer security ("TLS") messages.

1 4. The method of claim 1, wherein the secure communications
2 include internet protocol secure ("IPSec") techniques.

1 5. The method of claim 1, wherein evaluating the at least one
2 promise includes multiplying an inversion of a total product of the leaf nodes
3 with a partial product of the leaf nodes to produce the inversion of an individual
4 leaf node.

1 6. The method of claim 1, further comprising minimizing the
2 disparity among the sizes of the encryption exponents of the public keys within
3 the set.

1 7. The method of claim 1, wherein determining includes using a
2 plurality of separate, parallel batch trees finding the root node of each tree and
3 combining the final answers.

1 8. The method of claim 1, wherein decrypting includes
2 simultaneous multiple exponentiation such that the encryption exponents are
3 combined to reduce the number of exponentiations.

1 9. A method for improving secure communications in a computer
2 network comprising;
3 combining individually encrypted network security protection
4 handshake messages into a set of encrypted messages wherein each encrypted
5 handshake message is derived using a public key containing an encryption
6 exponent;
7 determining a root node of a binary tree comprising leaf nodes
8 corresponding to the encryption exponent of each encrypted message;
9 calculating a product of the encrypted messages;
10 extracting at least one root from the product of the encrypted messages;
11 and
12 decrypting the encrypted messages by evaluating at least one individual
13 leaf node by multiplying an inversion of the total product of leaf nodes with a
14 partial product of the leaf nodes to produce an inversion of the at least one
15 individual leaf node wherein efficiency of the decryption is increased.

1 10. The method of claim 9, wherein the network security protection
2 handshake messages include secure socket layer ("SSL") messages.

1 11. The method of claim 9, wherein the network security protection
2 messages include transport layer security ("TLS") messages.

1 12. The method of claim 9, wherein the network security protection
2 messages include internet protocol secure ("IPSec") messages.

1 13. The method of claim 9, further comprising minimizing the
2 disparity among the sizes of the encryption exponents of the public keys within
3 the set.

1 14. The method of claim 9, wherein determining includes using a
2 plurality of separate, parallel batch trees finding the root node of each tree and
3 combining the answers.

1 15. The method of claim 9, wherein decrypting includes
2 simultaneous multiple exponentiation such that the encryption exponents are
3 combined to reduce the number of exponentiations.

1 16. The method of claim 9, wherein decrypting includes expressing
2 the at least one root as at least one promise and evaluation the at least one
3 promise at the leaf nodes decreasing the number of modular inversions.

1 17. A method for secure communications in a computer network,
2 comprising;
3 combining individually encrypted network security protection
4 handshake messages into a set of encrypted messages wherein each encrypted
5 handshake message is derived using a public key containing an encryption
6 exponent;
7 determining a root node of a binary tree comprising leaf nodes
8 corresponding to the encryption exponent of each encrypted message;

9 calculating a product of the encrypted messages;
 10 extracting at least one root from the product of the encrypted messages;
 11 and
 12 decrypting the encrypted messages by minimizing the disparity between
 13 the sizes of the encryption exponents of the public keys, wherein efficiency of
 14 the secure communications is increased.

1 18. The method of claim 17, wherein combining includes secure
 2 socket layer ("SSL") messages.

1 19. The method of claim 17, wherein combining includes transport
 2 layer security ("TLS") messages.

1 20. The method of claim 17, wherein combining includes internet
 2 protocol secure ("IPSec") messages.

1 21. The method of claim 17, wherein determining uses a plurality of
 2 separate, parallel batch trees finding the root node of each tree and combining
 3 the final answers.

1 22. The method of claim 17, wherein decrypting includes
 2 simultaneous multiple exponentiation such that the encryption exponents are
 3 combined to reduce the number of exponentiations.

09072021060901
T08090"20E22850

1 23. The method of claim 17, wherein decrypting includes expressing
2 the at least one root as at least one promise and evaluating the at least one
3 promise at the leaf nodes decreasing the number of modular inversion.

1 24. The method of claim 17, wherein decrypting includes evaluating
2 at least one individual leaf node by multiplying an inversion of the total product
3 of leaf nodes with a partial product of the leaf nodes to produce an inversion of
4 the at least one individual leaf node.

1 25. A method for improving secure communications in a computer
2 network, comprising;
3 combining individually encrypted network security protection
4 handshake into a set of encrypted messages wherein each encrypted handshake
5 message is derived using a public key containing an encryption exponent;
6 determining a root node of a binary tree comprising leaf nodes
7 corresponding to each encryption exponent by using a plurality of separate
8 parallel batch trees finding the root node of each tree and combining the final
9 answers;
10 calculating a product of the encrypted messages;
11 extracting at least one root from the product of the encrypted messages;
12 and
13 decrypting the encrypted messages by expressing the at least one root as
14 at least one promise and evaluating the at least one promise at the leaf nodes

15 producing a reduced number of modular inversions wherein efficiency of
16 establishing secure communications is increased.

1 26. The method of claim 25, wherein combining includes secure
2 socket layer ("SSL") messages.

1 27. The method of claim 25, wherein combining includes transport
2 layer security ("TLS") messages.

1 28. The method of claim 25, wherein combining includes internet
2 protocol secure ("IPSec") messages.

1 29. The method of claim 25, wherein decrypting includes
2 simultaneous multiple exponentiation such that the encryption exponents are
3 combined to reduce the number of exponentiations.

1 30. The method of claim 25, wherein evaluating the at least one
2 promise includes multiplying an inversion of a total product of the leaf nodes
3 with a partial product of the leaf nodes to produce the inversion of an individual
4 leaf node.

1 31. The method of claim 25, further comprising minimizing the
2 disparity among the sizes of the encryption exponents of the public keys within
3 the set.

1 32. A method for secure communications in a computer network,
2 comprising;
3 combining individually encrypted network security protection messages
4 into a set of encrypted messages, wherein each encrypted handshake message is
5 derived using a public key containing an encryption exponent;
6 determining a root node of a binary tree comprising leaf nodes
7 corresponding to each encrypted messages encryption exponent;
8 calculating a product of the encrypted messages;
9 minimizing the disparity among the sizes of the encryption exponents of
10 the public keys within the set;
11 extracting at least one root from the product of the encrypted messages;
12 and
13 decrypting the encrypted messages by evaluating the at least one leaf
14 node by multiplying an inversion of a total product of the leaf nodes with a
15 partial product of the leaf nodes to produce the inversion of the at least one leaf
16 node wherein efficiency of establishing secure network communications is
17 increased.

1 33. The method of claim 32, wherein combining includes secure
2 socket layer ("SSL") messages.

1 34. The method of claim 32, wherein combining includes transport
2 layer security ("TLS") messages.

1 35. The method of claim 32, wherein combining includes internet
2 protocol secure ("IPSec") messages.

1 36. A method for secure communications in a computer network,
2 comprising:

3 coupling a client to a web server;

4 sending a client hello message to the web server;

5 generating a public / private key pair at the web server, wherein the
6 public key contains an encryption exponent;

7 responding to the client with a server hello message comprising the
8 public key;

9 encrypting a random handshake message at the client using the public
10 key;

11 sending the encrypted handshake message to a batch-decryption server;

12 batching handshake messages on a batch-decryption server according to
13 the public key such that the disparity between the sizes of the encryption
14 exponents of the public key is minimized;

15 separating the batch's e^{th} root in a downward-percolation phase into
16 constituent decrypted messages, wherein internal inversions are converted to
17 modular divisions increasing efficiency by producing a reduced number of
18 modular inversions;

19 scheduling the batch-decryption server based on server-load
20 considerations;

21 decrypting the handshake messages using at least one alternate

22 expression of at least on arithmetic function of at least one batch's e^{th} root; and
23 sending the decrypted message to the web server.

1 37. The method of claim 36, wherein batching handshake messages
2 includes Secure Socket Layer ("SSL") messages.

1 38. The method of claim 36, wherein combining includes transport
2 layer security ("TLS") messages.

1 39. The method of claim 36, wherein combining includes internet
2 protocol secure ("IPSec") messages.

1 40. The method of claim 36, wherein batching further comprises an
2 upward-percolation phase that combines individual encrypted messages to form
3 a value, v wherein v is the product of the individual encrypted messages raised
4 to the power of e/e_i , e being the product of all individual encryption exponents
5 e_i .

1 41. The method of claim 36, wherein the value v is determined by
2 the equation $v = \prod_{i=1}^b v_i^{e/e_i}$, where e is the product of individual
3 exponentiation exponents, v_i is the individual encrypted message, e_i is the
4 individual public key, and b is the number of encrypted messages in a particular
5 batch.

1 42. The method of claim 36, wherein batching further comprises an
2 exponentiation phase that includes the extraction of an e^{th} root from the value,
3 v.

1 43. The method of claim 36, wherein exponentiation further includes
2 simultaneous multiple exponentiation such that the encryption exponents are
3 combined to reduce the number of exponentiations.

1 44. The method of claim 36, wherein exponentiation includes
2 combining a plurality of inversions to form a single modular inversion.

1 45. The method of claim 36, wherein decrypting includes reducing
2 each encrypted batch message into a separate moduli, using separate parallel
3 batch trees to determine the moduli, and combining the final answers.

1 46. A method for batch decryption in a computer network
2 comprising:
3 combining a plurality of encrypted messages into a plurality of batches,
4 wherein each encrypted message includes a public / private key pair, each
5 public key comprising an encryption exponent;
6 scheduling the batches of encrypted messages using a plurality of
7 criteria selected from a group including maximum throughput, minimum
8 turnaround-time, minimum turnaround-time variance, and server load
9 considerations, wherein the efficiency of establishing secure communications is

10 enhanced; and
11 replacing at least one inversion of at least one batch decryption
12 operation with a single inversion and a plurality of multiplication operations,
13 wherein the speed of the decryption is significantly improved.

1 47. The method of claim 46, wherein combining a plurality of
2 encrypted messages includes secure socket layer ("SSL") messages.

1 48. The method of claim 46, wherein combining a plurality of
2 encrypted messages includes transport layer security ("TLS") messages.

1 49. The method of claim 46, wherein combining includes internet
2 protocol secure ("IPSec") messages.

1 50. The method of claim 46, further comprising using separate,
2 parallel batch trees and combining the results.

1 51. The method of claim 46, wherein combining includes selecting
2 the encrypted messages for the batches by balancing the encryption exponent.

1 52. A method for secure communications in a computer network,
2 comprising;
3 combining individually encrypted network security protection
4 handshake messages into a set of encrypted handshake messages wherein each

5 encrypted message is derived using a public key comprising an encryption
6 exponent;
7 determining a root node of a binary tree containing leaf nodes
8 corresponding to each encrypted message encryption exponent by using a
9 plurality of separate parallel batch trees finding the root node of each tree and
10 combining the final answers;
11 minimizing the disparity between the sizes of the encryption exponents
12 of the public keys within the set;
13 using simultaneous multiple exponentiation such that the encryption
14 exponents are combined to reduce the number of exponentiations;
15 calculating a product of the encrypted messages;
16 extracting at least one root from the product of the encrypted messages;
17 and
18 decrypting the encrypted messages by expressing the at least one root as
19 at least one promise and evaluating the at least one promise at the leaf nodes,
20 and multiplying an inversion of a total product of the leaf nodes with a partial
21 product of the leaf nodes decreasing the number of modular inversions by
22 producing an inversion of the leaf node wherein efficiency of secure
23 communications is increased.

1 53. The method of claim 52, wherein combining encrypted network
2 security protection handshake messages includes secure socket layer ("SSL")
3 messages.

1 54. The method of claim 52, wherein combining encrypted network
2 security protection handshake messages includes transport layer security
3 ("TLS") messages.

1 55. The method of claim 52, wherein combining encrypted network
2 security protection handshake messages includes internet protocol secure
3 ("IPSec") messages.

1 56. A method for performing batch decryption in a computer
2 network, comprising:
3 receiving a plurality of encrypted messages generated using a plurality
4 of public keys, wherein the plurality of public keys share a common modulus;
5 forming a binary tree using leaf nodes corresponding to the plurality of
6 public keys;
7 placing each of the plurality of encrypted messages in a leaf node having
8 a corresponding public key;
9 percolating the plurality of encrypted messages up the binary tree to
10 form a root node including a product of the encrypted messages, extracting at
11 least one root from the product of the encrypted messages by forming an
12 exponentiation product in the root node;
13 expressing the at least one root using at least one promise that includes
14 at least one alternative representation of at least one arithmetic function of the at
15 least one root;
16 percolating the at least one root down the binary tree using the at least

17 one promise; and

18 decrypting the plurality of encrypted messages by evaluating the at least
19 one promise at the leaf nodes, wherein efficiency of the decryption is increased
20 by reducing a number of modular inversions and a number of root extractions.

1 57. The method of claim 56, wherein receiving a plurality of
2 encrypted messages includes secure socket layer ("SSL") messages.

1 58. The method of claim 56, wherein receiving a plurality of
2 encrypted messages includes transport layer security ("TLS") messages.

1 59. The method of claim 56, wherein receiving a plurality of
2 encrypted messages includes internet protocol secure ("IPSec") messages.

1 60. The method of claim 56, wherein evaluating the at least one
2 promise uses batched division to calculate a plurality of inverses for the
3 plurality of leaf nodes using a single modular inversion, wherein the single
4 modular inversion is multiplied with a partial product at each leaf node to
5 produce a corresponding inverse for the leaf node

1 61. The method of claim 56, further comprising:
2 reducing each of the plurality of encrypted messages modulo p and q ;
3 generating two parallel batch trees modulo p and q ; and
4 batching in each of the two parallel batch trees modulo p and q .

1 62. The method of claim 56 , wherein the percolating includes
2 balanced exponents.

1 63. The method of claim 56, wherein the percolating includes
2 simultaneous multiple exponentiation.

1 64. A method for secure communications in a computer network,
2 comprising:
3 generating a Rivest-Shamir-Adleman ("RSA") public / private key pair
4 at a web server;
5 coupling a client to the web server;
6 sending a client hello message to the web server requesting the
7 establishment of a Secure Socket Layer ("SSL");
8 responding to the client with a server hello message containing the RSA
9 public key;
10 encrypting a random string R, the pre-master secret at the client, using
11 the RSA public key, wherein the resulting cipher-text, C, contains R;
12 sending the encrypted cipher-text message, C, to the web server;
13 combining individually encrypted secure socket layer ("SSL") encrypted
14 cipher-text messages to form a batch;
15 decrypting the batch of cipher-text, C, messages at the web server using
16 the RSA private keys to determine R, wherein the efficiency of the decryption is
17 enhanced by replacing at least one inversion with at least one multiplication;
18 and

19 establishing a common session key between the web server and the
20 client using R.

1 65. The method of claim 64, wherein decrypting includes using at
2 least one alternative representation of at least one arithmetic function to reduce
3 to the number of inversions.

1 66. A system for secure communications in a computer network
2 comprising:
3 at least one client processor;
4 at least one web server; and
5 at least one batch server coupled among the at least one client processor
6 and the at least one web server, wherein the at least one batch server receives
7 requests for decryption of a plurality of individually encrypted network secure
8 protection handshake messages, aggregates the plurality of individually
9 encrypted handshake messages into at least one batch wherein each encrypted
10 message is derived by using an encryption exponent from an Rivest-Shamir-
11 Adleman ("RSA") public / private key pair, forms a binary tree containing leaf
12 nodes corresponding to each encryption exponent, extracts at least one root
13 from a product of the encrypted messages, decrypts the encrypted messages by
14 expressing the at least one root as at least one promise and evaluating the at
15 least one promise at the leaf nodes, and multiplies an inversion of a total
16 product of the leaf nodes with a partial product of the leaf nodes producing an

17 inversion of the leaf node decreasing the number of modular inversions, and
18 responds to the requests for decryption with corresponding plain-text.

1 67. The system of claim 66, wherein the individually encrypted
2 network secure protection handshake messages includes secure socket layer
3 ("SSL") messages.

1 68. The system of claim 66, wherein the individually encrypted
2 network secure protection handshake messages includes transport layer security
3 ("TLS") messages.

1 69. The method of claim 66, wherein the individually encrypted
2 network secure protection handshake messages includes internet protocol secure
3 ("IPSec") messages.

1 70. The system of claim 66, wherein the batch server aggregates the
2 plurality of encrypted messages base on criteria including maximum
3 throughput, minimum turnaround time, and minimum turnaround time variance.

1 71. A system for secure communications in a computer network,
2 comprising at least one client processor coupled among at least one web server,
3 wherein the web server receives requests for decryption of a plurality of
4 individually encrypted network security protection handshake messages,
5 aggregates the plurality of individually encrypted handshake messages into at

6 least one batch wherein each encrypted message is derived using an encryption
7 exponent from an Rivest-Shamir-Adleman ("RSA") public / private key pair,
8 forms a binary tree containing leaf nodes corresponding to each encryption
9 exponent, extracts at least one root from a product of the encrypted messages,
10 decrypts the encrypted messages by expressing the at least one root as at least
11 one promise and evaluating the at least one promise at the leaf nodes, and
12 multiplies an inversion of a total product of the leaf nodes with a partial product
13 of the leaf nodes producing an inversion of the leaf node decreasing the number
14 of modular inversions, wherein efficiency of secure communications is
15 increased.

1 72. A system of scheduling batch decryption in a computer network,
2 comprising:
3 a plurality of client processors;
4 at least one web server;
5 at least one batch server coupled among the at least one web server and
6 the plurality of client processors using a Rivest-Shamir-Adleman ("RSA")
7 decryption algorithm, wherein the at least one batch server links the plurality of
8 client processors to the at least one web server; and
9 a scheduler, wherein during a timed period the scheduler places arriving
10 encrypted messages in a queue forming a batch, wherein the encrypted
11 messages in the queue are decrypted upon completion of the timed period.

1 73. A system for secure network communications in a computer
2 network, comprising at least one batch server coupled among at least one client
3 processor and at least one web server, wherein the at least one batch server uses
4 a Rivest-Shamir-Adleman ("RSA") batch algorithm to decrypt an aggregation
5 of encrypted messages transferred among the at least one client processor and
6 the at least one web server.

1 74. A system for secure computer network communications,
2 comprising at least one client processor and at least one server processor
3 wherein the server processor combines decryption requests of Secure Socket
4 Layer ("SSL") messages into at least one batch and decrypts the at least one
5 batch using a Rivest-Shamir-Adleman ("RSA") batch decryption algorithm.

1 75. A computer-readable medium, comprising executable
2 instructions for establishing secure communications in a computer network
3 which, when executed in a processing system, causes the system to:
4 combine individually encrypted network security protection handshake
5 messages into a set of encrypted messages wherein each encrypted handshake
6 message is derived using a public key comprising an encryption exponent;
7 determine a root node of a binary tree containing leaf nodes
8 corresponding to each encrypted messages encryption exponent by using a
9 plurality of separate parallel batch trees to find the root node of each tree and
10 combine the final answers;
11 minimize the disparity between the sizes of the encryption exponents of

12 the public keys within the set;
 13 combine the encryption exponents using simultaneous multiple
 14 exponentiation such that the number of exponentiations is reduced;
 15 calculate a product of the encrypted messages;
 16 extract at least one root from the product of the encrypted messages; and
 17 decrypt the encrypted messages by expressing the at least one root as at
 18 least one promise and evaluating the at least one promise at the leaf nodes,
 19 multiplying an inversion of a total product of the leaf nodes with a partial
 20 product of the leaf nodes producing an inversion of the leaf node and decreasing
 21 the number of modular inversions, wherein efficiency of establishing secure
 22 communications is increased.

1 76. An electromagnetic medium, comprising executable instructions
 2 for establishing secure communications in a computer network which, when
 3 executed in a processing system, causes the system to;
 4 combine individually encrypted secure network handshake messages
 5 into a set of encrypted handshake messages wherein each encrypted handshake
 6 message is derived using a public key comprising an encryption exponent;
 7 determine a root node of a binary tree containing leaf nodes
 8 corresponding to each encrypted messages encryption exponent by using a
 9 plurality of separate parallel batch trees to find the root node of each tree and
 10 combine the final answers;
 11 minimize the disparity between the sizes of the encryption exponents of
 12 the public keys within the set;

13 combine the encryption exponents using simultaneous multiple
14 exponentiation such that the number of exponentiations is reduced;
15 calculate a product of the encrypted messages;
16 extract at least one root from the product of the encrypted messages; and
17 decrypt the encrypted messages by expressing the at least one root as at
18 least one promise and evaluating the at least one promise at the leaf nodes,
19 multiplying an inversion of a total product of the leaf nodes with a partial
20 product of the leaf nodes producing an inversion of the leaf node, and
21 decreasing the number of modular inversions wherein efficiency of establishing
22 secure communications is increased.